

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Savage et al.	Examiner:	Doan
Title:	System for Providing Session-Based Network Privacy, Private, Persistent Storage, and Discretionary Access Control for Sharing Private Data		
Filing Date:	10/28/2003	Serial No.:	10/695,507 (Continuation of PCT/US02/08275)
Ref. No.:	14137.0001 (B)	Group Art Unit:	2131

AMENDMENT

To: Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This amendment is in response to an Office Action mailed on March 2, 2007, in connection with the above-referenced patent application. Applicant respectfully requests a one-month extension to reply. Applicant submits herewith a credit card payment of the required extension fee. Applicant authorizes any additional fees to be charged to Hughes Hubbard & Reed Deposit Account No. 08-3264.

Please amend the application as follows:

Amendments to the Claims begin on page 2 herein.

Remarks begin on page 5 herein.

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

1. (currently amended) A method for providing session protection for user privacy over a network, by means including at least a client and a remote server, wherein a user, using a client application, may submit a request through said client for a specified action to be performed in response to said request by said remote server, said user-submitted request comprising identity information that identifies the user making the request, and action information that specifies the action requested from said remote server by said user, wherein said communications are provided in a secure and anonymous manner in that said action information is submitted to said remote server without revealing said identity information to said remote server, and in that only said client, and not any facility through which said action information or any response thereto passes in the course of being submitted to or received from said remote server, possesses both said identity information and said action information, said system comprising (in addition to said client and remote server):
 - (a) separating, within said client application, said identity information and said action information from the user's information request, encrypting said action information, and sending said identity information and said action information as so encrypted to an identity server;
 - (b) transmitting said encrypted action information from said identity server to an action server;
 - ~~(b)~~ decrypting, within said ~~second-intermediate action~~ action server, said action information, transmitting said decrypted action information to said remote server, receiving the remote server's response, encrypting said remote server response, and transmitting said encrypted remote server response to said ~~first-intermediate identity~~ identity server;
 - ~~(d)~~ receiving, within said ~~first-intermediate identity~~ identity server said encrypted remote server response from said ~~second-intermediate action~~ action server, associating said encrypted remote

server response with said identity information and sending said encrypted remote server response to said application; and

(de) decrypting, within said client application, said remote server response and forwarding said decrypted remote server response to said client for presentation to said user.

2. (canceled without prejudice)

3. (canceled without prejudice)

4. (canceled without prejudice)

5. (canceled without prejudice)

6. (canceled without prejudice)

7. (canceled without prejudice)

8. (canceled without prejudice)

9. (canceled without prejudice)

10. (currently amended) ~~The method of any of claims 2,3,4, 5,6,7 or 8, wherein said server is a second intermediate server in a system comprising first and second intermediate servers adapted to perform the method of claim 1, and wherein data transfer to and from said second intermediate server is conducted through a first intermediate server in accordance with the method of claim 1.~~ The method of claim 1, adapted to provide private storage of data within a network, to a user operating a computer connected to said network, said computer having a client application resident therein, there being available to said user on said network a server to provide storage services, said server being an action server in a system comprising an identity server and an action server in accordance with claim 1, said method for providing private storage comprising:

(a) generating within said client application a first encryption key and a first decryption key;

(b) encrypting said data within said client using said first encryption key;

(c) generating a data object identifier within said client application;

(d) creating a data object that contains said data object identifier and said encrypted data;

- (e) sending said data object to said server;
- (f) storing said data object in a database under the control of said server, using said data object identifier as a locator;
- (g) writing said data object identifier to a user object within said client application;
- (h) writing said first decryption key to said user object;
- (i) generating within said client application a user object encryption key based on information private to said user and reproducible in future sessions by said user, in a manner such that said private information cannot practicably be derived from said user object encryption key;
- (j) encrypting said user object with said user object encryption key;
- (k) generating within said client application a user object identifier based on information private to said user and reproducible in future sessions by said user, in a manner such that said private information cannot practicably be derived from said user object identifier;
- (l) associating said user object identifier with said user object;
- (m) sending said user object and user object identifier to said server; and
- (n) storing said user object in said database, using said user object identifier as a locator.

11. (previously amended) The method of claim 1 wherein said identity server and said action server are implemented as processes or threads which may execute on the same or different computers.
12. (currently amended) The method of claim 10 carried out in a distributed operating environment in which there are a plurality of users, a plurality of first-intermediate identity servers and a plurality of second-intermediate action servers, all communicating in accordance with the method of claim 1.
13. (previously presented) The method of claim 10 wherein said identity server and said action server are implemented as processes or threads which may execute on the same or different computers.

REMARKS

In the Office Action dated March 2, 2007, the Examiner determined that the application covers the following 2 inventions:

Invention I: Claims 1 and 10 – 13.

Invention II: Claims 2 – 9.

The Examiner required that Applicant choose one invention for examination purposes under 35 U.S.C. § 121.

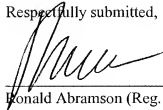
Applicant hereby elects, without traverse, Invention I which consists of claims 1 and 10 – 13 for prosecution on the merits. Applicant reserves the right to file divisional applications for the non-elected invention at a later date.

CONCLUSION

In view of the foregoing, Applicant respectfully requests that Invention I be considered on the merits.

Dated: April 11, 2007

Respectfully submitted,



Ronald Abramson (Reg. No. 34,762)

HUGHES HUBBARD & REED LLP
One Battery Park Plaza
New York, New York 10004-1482
212-837-6404